(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平7－327029**

(43)公開日　平成７年(1995)12月12日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|
| Ｈ０４Ｌ 9/06 | | | | |
| 9/14 | | | | |
| Ｇ０９Ｃ 1/00 | | 9364－5Ｌ | | |
| | | | Ｈ０４Ｌ 9/02 | Ｚ |

審査請求　未請求　請求項の数13　ＯＬ　（全 16 頁）

(21)出願番号　特願平6－117828

(22)出願日　平成６年(1994)５月31日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　上野　知行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　瀬田　満
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

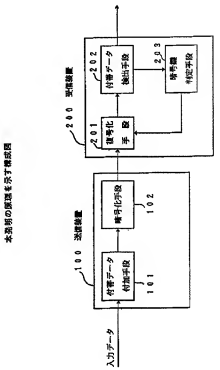
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　暗号化通信システム

(57)【要約】

【目的】　データを暗号化するために使用する暗号鍵を複数個持ち、これらの１つを随時切り替えて使用するような暗号化通信システムに関し、受信側に暗号鍵番号が正しく通知されなくても受信側で訂正可能にすることを目的とする。

【構成】　送信装置１００において、暗号化すべきデータに何らかの付帯データを付加する付帯データ付加手段１０１を備え、受信装置２００には復号した後のデータからその付帯データを検出する付帯データ検出手段２０２と、その付帯データが正常に検出できないときに、受信装置２００の暗号鍵を順次変更する暗号鍵判定手段２０３とを備えるようにした。これにより、暗号鍵の変更時などに、暗号鍵の番号が正常に通知されなくても、受信側のみで回復することができるようになる。



【特許請求の範囲】

【請求項１】　必要に応じて随時切り替えて使用される複数の暗号鍵を持った暗号化通信システムにおいて、
暗号化すべき入力データに付帯データを付加する付帯データ付加手段（１０１）及び切り替えて使用される複数の暗号鍵を有し、前記付帯データ付加手段より出力される前記入力データ及び付帯データに対して暗号化を行う暗号化手段（１０２）を備えた送信装置（１００）と、
伝送路を介して受信された暗号化データを復号する復号化手段（２０１）、入力データに付加されていた付帯データを検出する付帯データ検出手段（２０２）、及び検出された付帯データの誤り率に応じて復号化に使用した暗号鍵が正しいかどうかを判定し、前記暗号鍵が正しくないと判定したときには前記復号化手段に対し復号化に使用する暗号鍵を変更するよう指示する暗号鍵判定手段（２０３）を備えた受信装置（２００）と、
から構成されることを特徴とする暗号化通信システム。

【請求項２】　前記暗号化手段（１０２）は設定された暗号鍵に従って前記付帯データ付加手段からの前記入力データ及び付帯データを暗号化する手段及び暗号化したデータに暗号化に使用した暗号鍵の番号を多重化する手段を備え、前記復号化手段（２０１）は受信されたデータから暗号鍵の番号を分離して復号に使用する暗号鍵の番号を取得し、前記暗号鍵判定手段から暗号鍵が正しくないとの判定結果に応答して前記暗号鍵の番号を変更する手段を備えていることを特徴とする請求項１記載の暗号化通信システム。

【請求項３】　前記付帯データ付加手段（１０１）は入力データを誤り検出符号によって符号化する誤り検出符号化部とし、前記付帯データ検出手段（２０２）は前記復号化手段によって復号化された誤り検出符号を検査する誤り検出部とすることを特徴とする請求項１記載の暗号化通信システム。

【請求項４】　前記付帯データ付加手段（１０１）は入力データにユニークワードを付加するユニークワード付加部とし、前記付帯データ検出手段（２０２）は前記復号化手段によって復号化されたユニークワードを検査するユニークワード検出部とすることを特徴とする請求項１記載の暗号化通信システム。

【請求項５】　必要に応じて随時切り替えて使用される複数の暗号鍵を持った暗号化通信システムの受信装置において、
伝送路を介して受信された暗号化データを予め設定した暗号鍵によって復号する復号化手段（２０１）と、
復号化されたデータから入力データに付加されていた付帯データを検出する付帯データ検出手段（２０２）と、
検出された付帯データの誤り率に応じて復号化に使用した暗号鍵が正しいかどうかを判定し、暗号鍵が正しくないときには前記復号化手段の暗号鍵を変更させる暗号鍵判定手段（２０３）と、
を備えていることを特徴とする受信装置

【請求項６】　前記復号化手段（２０１）は、伝送路を介して伝送されてきた暗号化データを入力して指定された暗号鍵により復号化するデータ復号化部と、送信装置の暗号鍵テーブルと同じ内容を有する暗号鍵テーブルとを備えていることを特徴とする請求項５記載の受信装置。

【請求項７】　前記復号化手段（２０１）は、伝送路を介して伝送されてきた暗号化データを入力して暗号化データから暗号鍵番号を分離する分離部と、分離された暗号鍵番号を受信する暗号鍵番号受信部とをさらに備えていることを特徴とする請求項６記載の受信装置。

【請求項８】　前記付帯データ検出手段（２０２）は、前記復号化手段によって復号化された誤り検出符号を検査する誤り検出部であることを特徴とする請求項５記載の受信装置。

【請求項９】　前記暗号鍵判定手段（２０３）は、前記誤り検出部にて検出された誤り率に応じて復号に使用する暗号鍵を変更させる暗号鍵判定部であることを特徴とする請求項５記載の受信装置。

【請求項１０】　前記暗号鍵判定部は、前記付帯データ検出手段にて検出した情報を基にして誤り率を算出する誤り率計算手段と、算出された誤り率が所定の値を越えたときに復号化に使用した暗号鍵は異常であると判定する判定手段と、暗号鍵が異常であると判定されたときに複数用意された暗号鍵番号を順次切り替える鍵番号切替手段とから構成されることを特徴とする請求項９記載の受信装置。

【請求項１１】　前記付帯データ検出手段（２０２）、は前記復号化手段によって復号化されたユニークワードを検査するユニークワード検出部であることを特徴とする請求項５記載の受信装置。

【請求項１２】　前記暗号鍵判定手段（２０３）は、前記ユニークワード検出部にて検出されたユニークワードの不検出率に応じて復号に使用する暗号鍵を変更させる暗号鍵判定部であることを特徴とする請求項５記載の受信装置。

【請求項１３】　受信された暗号化データを蓄積する受信バッファ手段と、前記復号化手段によって復号化されたデータを蓄積する出力バッファ手段と、前記受信バッファ手段に、前記復号化手段への受信データの転送を指示するとともに復号されたデータが正常の場合にその復号化済みのデータを削除する指示を出し、前記出力バッファ手段には復号されたデータが正常の場合にそのデータを有効データとして出力する指示を出すバッファ制御手段とをさらに備えていることを特徴とする請求項５記載の受信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は暗号化通信システムに関

し、特にデータを暗号化するために使用する暗号鍵を複数個持ち、これら暗号鍵を必要に応じて切り替えて使用するようなデータ通信システムにおける暗号化通信システムに関する。

【０００２】従来、通信回線上を伝送するデータが傍受されてもそのデータの意味する内容が分からないようにするために、機密保持の必要なデータは暗号化して伝送するという方法が取られている。暗号化方式には、ＤＥＳ（Data Encryption Standard）、ＦＥＡＬ（Fast data Encipherment ALgorithm）などの秘密及び公開の暗号鍵を使用する方法があり、送信側と受信側とで同じ暗号鍵を用いて正常なデータ通信が行われる。

【０００３】

【従来の技術】図１６は従来の暗号化通信システムの構成を示す図である。図において、従来の暗号化通信システムはデータを暗号化して送るための送信装置１とその暗号化データを受けて復号するための受信装置２とで構成される。送信装置１と受信装置２との間の伝送路３は、特に規定はしないが、たとえば電話線のような有線の形態をとるものであったり、衛星を利用した通信のような無線の形態をとるものであったりする。なお、図示の送信装置１及び受信装置２は暗号化に係わる部分についてのみ示してある。

【０００４】送信装置１は、入力データを暗号鍵ｋｓにより暗号化するデータ暗号化部１１と、指定された番号Ｎ（ｋｓ）から暗号鍵ｋｓに変換する暗号鍵テーブル１２と、入力データを暗号化するために暗号鍵テーブル１２のどの暗号鍵ｋｓを使用するかを番号Ｎ（ｋｓ）で選択する暗号鍵番号設定部１３と、暗号鍵番号設定部１３で選択した暗号鍵番号Ｎ（ｋｓ）を受信装置２へ送るための暗号鍵番号送出部１４と、暗号化されたデータと暗号鍵番号Ｎ（ｋｓ）とを多重化する多重化部１５とから構成される。

【０００５】一方、受信装置２は、伝送路３を介して伝送されてきた暗号化データを入力して暗号化データと暗号鍵番号とに分離する分離部２１と、分離された暗号鍵番号を受信する暗号鍵番号受信部２２と、送信装置１の暗号鍵テーブル１２と同じ内容を有する暗号鍵テーブル２３と、分離された暗号化データを暗号鍵番号Ｎ（ｋｓ）′で指定された暗号鍵ｋｓにより復号化するデータ復号化部２４とから構成される。

【０００６】送信装置１及び受信装置２は複数の暗号鍵を有する同一の暗号鍵テーブル１２，２３を持ち、受信装置２に対しては伝送するデータの暗号化に使用した暗号鍵に対応する暗号鍵番号のみを伝送するようにし、受信側ではそれを解読して暗号鍵番号を取得し、この暗号鍵番号から送信側と同じ暗号鍵を取り出して暗号化されたデータを復号するようにしている。この構成によれば、暗号鍵番号は随時変更することが可能であり、また、暗号鍵そのものを伝送しないので秘匿性の高い伝送路を確保するものである。

【０００７】図１７は従来の暗号化通信システムの伝送路上のデータイメージを示す図である。この図によれば、送信装置１から送出された伝送路３上のデータは、データ暗号化部１１によって暗号化されたＤと、暗号鍵番号送出部１４より出力されて多重化部１５で多重化された暗号鍵番号Ｎ（ｋｓ）と、フレーム同期信号Ｆとで構成される。暗号鍵番号Ｎ（ｋｓ）は通常、その変更時のみ送られるようにしているが、データ通信開始時のみ、一定周期毎、あるいはフレーム毎に常に送るようにすることもある。

【０００８】

【発明が解決しようとする課題】しかし、複数の暗号鍵を持つ従来の暗号化通信システムでは、送信装置から受信装置に対して暗号鍵番号の情報を送るようにしているので、たとえば、暗号鍵番号変更時に送出したデータのうち、たまたまその暗号鍵番号に関する情報が１つ誤ってしまった場合には、先に通知されていた暗号鍵番号に対応する暗号鍵で復号するため、他のデータまですべて誤ってしまい、正しい復号ができなくなる。しかもこのような場合、暗号鍵番号が正しく通知されるまでは、受信したデータはすべて異常となる。

【０００９】また、双方向型の通信システムであれば、暗号鍵が異なっていることが検出されれば、暗号鍵番号の再送を要求することもできるが、放送などの片方向型通信システムの場合は、再送要求ができないために、暗号鍵番号が正しく通知されるまでの間は、受信データはすべて異常となる。

【００１０】本発明はこのような点に鑑みてなされたものであり、複数の暗号鍵を使用し、暗号鍵番号を暗号鍵変更時のような間隔でしか伝送されないような場合において、暗号鍵番号が誤って通知されても正しい暗号鍵番号に訂正する暗号化通信システムを提供することを目的とする。

【００１１】また、本発明は、暗号鍵番号自体を送らなくても、送信側と同じ暗号鍵番号を受信側で見つけ出し、暗号鍵に変更があった場合にもそれに追随して送信側と同じ暗号鍵番号に訂正する暗号化通信システムを提供することを目的とする。

【００１２】さらに本発明は、送信されたデータはすべて誤りなく受信することができる暗号化通信システムを提供することを目的とする。

【００１３】

【課題を解決するための手段】図１は上記目的を達成する本発明の原理を示す構成図である。この図において、送信装置１００は、暗号化すべき入力データに付帯データを付加する付帯データ付加手段１０１と、切り替えて使用される複数の暗号鍵を有し、付帯データ付加手段１０１より出力される入力データ及び付帯データに対して暗号化を行う暗号化手段１０２とで構成される。一方、

受信装置２００は、伝送路を介して受信された暗号化データを復号する復号化手段２０１と、入力データに付加されていた付帯データを検出する付帯データ検出手段２０２と、検出された付帯データの誤り率に応じて復号化に使用する暗号鍵を変更するよう復号化手段２０１に対して指示する暗号鍵判定手段２０３とで構成される。

【００１４】

【作用】上述の手段によれば、送信装置１００において、暗号化すべき入力データに対して伝送路で誤りを発生した場合に識別できるような付帯データを付加してから、これらデータを暗号化手段１０２にて暗号化する。暗号化手段１０２は、複数の暗号鍵を持つテーブルを備えており、必要に応じて暗号化に使用する暗号鍵を随時切り替えるようにする。受信装置２００においては、復号化手段２０１にて受信データが復号化され、さらに付帯データ検出手段２０２では復号化されたデータから付帯データを検出する。暗号鍵判定手段２０３は、まず、検出された付帯データの誤り率を計算し、その誤り率が少ない場合は伝送路にて生じた誤りであると判定し、誤り率が所定の値を越えたならば、復号化手段２０１で使用している暗号鍵は誤っていると判定して復号化手段２０１に対して違う暗号鍵を使用するよう指示する。

【００１５】

【実施例】最初に、本発明の実施例の概要について説明する。図１は本発明の原理を示す構成図である。本発明の暗号化通信システムによれば、送信装置１００は、暗号化すべき入力データに付帯データを付加する付帯データ付加手段１０１と、付帯データ付加手段１０１より出力される入力データ及び付帯データに対して暗号化を行う暗号化手段１０２とで構成され、受信装置２００は、伝送路を介して受信された暗号化データを復号する復号化手段２０１と、入力データに付加されていた付帯データを検出する付帯データ検出手段２０２と、検出された付帯データの誤り率に応じて復号化に使用する暗号鍵を変更するよう復号化手段２０１に対して指示する暗号鍵判定手段２０３とで構成されている。

【００１６】まず、送信装置１００においては、暗号化すべき入力データに対して伝送路で誤りを発生した場合に識別できるような付帯データを付加してから、これらデータを暗号化手段１０２にて暗号化する。暗号化手段１０２は、複数の暗号鍵を持つテーブルを備えており、必要に応じて暗号化に使用する暗号鍵を随時切り替えるようにする。受信装置２００においては、復号化手段２０１にて受信データが復号化され、さらに付帯データ検出手段２０２では復号化されたデータから付帯データを検出する。暗号鍵判定手段２０３は、まず、検出された付帯データの誤り率を計算し、その誤り率が少ない場合は伝送路にて生じた誤りであると判定し、誤り率が所定の値を越えたならば、復号化手段２０１で使用している暗号鍵は誤っていると判定して復号化手段２０１に対して違う暗号鍵を使用するよう指示する。これにより、受信装置側では常に正しい暗号鍵が選択使用されることになる。

【００１７】図２は本発明の暗号化通信システムの第１実施例を示す構成図である。この図において、本発明の暗号化通信システムは、送信装置１００と、受信装置２００と、これらの間の通信回線とする伝送路３００とで構成される。

【００１８】送信装置１００は、入力データを受けてこの入力データに誤り検出符号を符号化して付加する誤り検出符号化部１１０を有している。この誤り検出符号化部１１０は、図１に示した原理図の付帯データ付加手段１０１に相当するもので、誤り検出符号とともに、たとえば、パリティ検査符号、ＢＣＨ（Bose-Chaudhuri-Hocquenghem）符号、畳込み符号などの誤り検出訂正符号が使用される。送信装置１００はさらに、入力データを暗号鍵ｋｓにより暗号化するデータ暗号化部１１１と、指定された番号Ｎ（ｋｓ）から暗号鍵ｋｓに変換する暗号鍵テーブル１１２と、入力データを暗号化するために暗号鍵テーブル１１２のどの暗号鍵ｋｓを使用するかを番号Ｎ（ｋｓ）で選択する暗号鍵番号設定部１１３と、暗号鍵番号設定部１１３で選択した暗号鍵番号Ｎ（ｋｓ）を受信装置２００へ通知するための暗号鍵番号送出部１１４と、暗号化されたデータと暗号鍵番号Ｎ（ｋｓ）とを多重化する多重化部１１５とを有し、これらの構成は図１に示した原理図の暗号化手段１０２に相当する。

【００１９】受信装置２００は、伝送路３００を介して伝送されてきた暗号化データを入力して暗号化データと暗号鍵番号とに分離する分離部２１０と、分離された暗号鍵番号を受信する暗号鍵番号受信部２１１と、送信装置１００の暗号鍵テーブル１１２と同じ内容を有する暗号鍵テーブル２１２と、分離された暗号化データを指定された暗号鍵ｋｓにより復号化するデータ復号化部２１３とを有している。これらの構成は図１に示した原理図の復号化手段２０１に相当する。受信装置２００はさらに、データ復号化部２１３にて復号されたデータの中から誤り検出符号を検出してどのビットが誤っているかを検出する誤り検出部２１４と、この誤り検出部２１４にて一定時間内に検出された誤りの数、すなわち誤り率に応じて、復号に使用している暗号鍵を変更させる暗号鍵判定部２１５とを有している。誤り検出部２１４は、図１の付帯データ検出手段２０２に相当し、暗号鍵判定部２１５は暗号鍵判定手段２０３に相当する。

【００２０】このように、送信装置１００及び受信装置２００には、暗号鍵を予め複数個用意し、各暗号鍵に対しては暗号鍵番号を付与して、それらの対応表である暗号鍵テーブル１１２及び２１２に入れている。暗号鍵の変更を行う場合には、予め準備されている暗号鍵の中から１つの暗号鍵ｋｓを送信装置１００の暗号鍵番号設定部１１３にて暗号鍵番号Ｎ（ｋｓ）で選択する。選択さ

れた暗号鍵番号Ｎ（ｋｓ）は暗号鍵テーブル１１２にて暗号鍵番号ｋｓに変換され、データ暗号化部１１１で使用されるとともに、暗号鍵番号送出部１１４及び多重化部１１５を介して受信側に通知される。また、入力データには、誤り検出符号化部１１０にて誤り検出符号が付加されて、データ暗号化部１１１で暗号化される。

【００２１】受信装置２００では、分離部２１０にて、多重化された暗号鍵番号が分離され、暗号鍵番号受信部２１１にて受信される。受信された暗号鍵番号は伝送路３００にて誤っている可能性があるため、Ｎ（ｋｓ）′で示してある。暗号鍵判定部２１５においてはまず、受信された暗号鍵番号Ｎ（ｋｓ）′は正しい暗号鍵番号Ｎ（ｋｓ）であるとして、その暗号鍵番号Ｎ（ｋｓ）により暗号鍵テーブル２１２が参照されて対応する暗号鍵ｋｓが選択され、データ復号化部２１３ではこの暗号鍵ｋｓによる復号が行われる。誤り検出部２１４では、誤り検出符号を使用してデータ復号化部２１３にて復号化された誤り検出符号化データに誤りがあるかどうかを検出する。誤りが検出されれば、誤り検出部２１４は誤り検出情報ＥＲＲを出力する。暗号鍵判定部２１５では、誤り検出部２１４からの誤り検出情報ＥＲＲを受けて、その情報が伝送路３００で偶発的に生じたものなのか、暗号鍵が誤っていることにより生じたものなのかを判断し、誤り率が高くて暗号鍵が誤っているいると思われる場合には、暗号鍵番号を変更し、その暗号鍵番号に対応する暗号鍵を使用して復号化を試みる。この暗号鍵番号の変更は、誤り検出部２１４での誤りがなくなるか予め定めた誤り率以下になるまで繰り返される。

【００２２】図３は暗号鍵判定部の一例を示す構成図である。この図において、暗号鍵判定部２１５は、誤り検出部２１４からの誤り検出情報ＥＲＲを受ける誤り率計算部２１５１と、誤り率設定部２１５２と、判定部２１５３と、暗号鍵番号受信部２１１で受信した暗号鍵番号Ｎ（ｋｓ）′を受けた時にこれを保持して暗号鍵番号Ｎ（ｋｓ）として暗号鍵テーブル２１２に与える鍵番号切替部２１５４とで構成される。

【００２３】誤り率計算部２１５１は誤り検出部２１４からの誤り検出情報ＥＲＲを受けて誤り率を計算する。判定部２１５３は、誤り率計算部２１５１で計算された誤り率と誤り率設定部２１５２で設定された誤り率とを比較し、誤り率が低い場合は伝送路３００上で伝送誤りが発生したと判定し、誤り率が設定された誤り率より高いとデータ復号化部２１３で使用している暗号鍵が間違っていると判定する。暗号鍵が間違っていると判定された場合には、鍵番号切替部２１５４は、暗号鍵番号受信部２１１で受信した暗号鍵番号Ｎ（ｋｓ）′に対応する暗号鍵番号を別の暗号鍵番号に切り替える。たとえば、暗号鍵番号Ｎ（ｋｓ）′の入力を受けて暗号鍵番号Ｎ（ｋｓ）＝１を出力していたとすると、暗号鍵番号Ｎ（ｋｓ）＝２を出力する。この切り替えは、予め用意された複数の暗号鍵に対応する暗号鍵番号の範囲内で順次行われ、誤り率が誤り率設定部２１５２で設定した値以下になるまで繰り返される。

【００２４】図４は第１実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。この図によれば、伝送路３００に送出されるデータは、送信装置１００に入力されたデータＤに誤り検出符号化部１１０にてチェックビットＣＨＫが付加されて誤り検出符号化され、この符号化されたデータが暗号化されている。この暗号化されたデータにはフレーム同期信号Ｆが付加されている。さらに、送信装置１００の暗号鍵番号設定部１１３により暗号鍵番号が変更された場合には、図示のように、たとえばデータＤの先頭に、設定変更された暗号鍵番号Ｎ（ｋｓ）が挿入されて送られる。

【００２５】図５は本発明の暗号化通信システムの第２実施例を示す構成図である。この実施例は第１実施例と比較して、誤り検出符号を使用する代わりにユニークワードを使用している点が相違する。

【００２６】すなわち、送信装置１００は、入力データを受けてこの入力データにユニークワードを付加するユニークワード付加部１２０を有している。ユニークワードは、一般には他のデータとは差が大きくて他のデータにはあり得ないようなある決められたビット数からなる特定パターンのビット並びを有するデータであって、しかも、１ビットが誤っていても、全体を見れば、ユニークワードであることが想像することができるような値を有しているワードである。

【００２７】送信装置１００は、ユニークワード付加部１２０の他は第１実施例の構成と同じであり、データ暗号化部１１１と、暗号鍵テーブル１１２と、暗号鍵番号設定部１１３と、暗号鍵番号送出部１１４と、多重化部１１５とを有している。

【００２８】一方、受信装置２００では、分離部２１０と、暗号鍵番号受信部２１１と、送信装置１００の暗号鍵テーブル１１２と同じ内容の暗号鍵テーブル２１２と、データ復号化部２１３とが第１実施例の構成と同じであり、これに、ユニークワード検出部２２４及び暗号鍵判定部２２５が備えられている。

【００２９】この実施例では、入力データ全体に誤り検出のための符号化を行うのではなく、送信側で入力データに単にユニークワードを付加したものを暗号化して送り、受信側では復号化したデータからそのユニークワードが正しく検出されることを以て、使用している暗号鍵は正しいと判断するようにしている。ユニークワードの検出は受信装置２００のユニークワード検出部２２４にて行われ、ユニークワードが検出された場合にユニークワード検出情報ＤＥＤを出力する。ユニークワードが正しく検出されない場合には、ユニークワード検出情報ＤＥＤはユニークワード不検出を表す情報となる。暗号鍵判定部２２５では、そのユニークワード検出情報ＤＥＤ

を受けて、ユニークワードが検出できない割合、すなわちユニークワードの不検出率を計算する。ユニークワードの不検出率が増えてくると、その原因は伝送路３００の誤りではなく暗号鍵の相違によるものと判定して、暗号鍵番号の変更をするようにする。

【００３０】図６は第２実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。この図によれば、伝送路３００に送出されるデータは、ユニークワード付加部１２０にて送信装置１００に入力されたデータＤの先頭に単純にユニークワードＵＷが付加され、この付加されたデータが暗号化されている。この暗号化されたデータにはフレーム同期信号Ｆが付加されている。さらに、送信装置１００の暗号鍵番号設定部１１３により暗号鍵番号が変更された場合には、図示のように、暗号化されたデータの、たとえば先頭に、変更された暗号鍵番号Ｎ（ｋｓ）が挿入されて送られる。

【００３１】図７は本発明の暗号化通信システムの第３実施例を示す構成図である。この実施例は第１実施例と比較して、暗号鍵番号設定部１１３にて選択された暗号鍵番号を受信側に送出しない点が相違する。

【００３２】すなわち、送信装置１００は、入力データを受けてこの入力データに誤り検出符号を符号化して付加する誤り検出符号化部１１０と、入力データを暗号鍵ｋｓにより暗号化するデータ暗号化部１１１と、指定された番号Ｎ（ｋｓ）から暗号鍵ｋｓに変換する暗号鍵テーブル１１２と、入力データを暗号化するために暗号鍵テーブル１１２のどの暗号鍵ｋｓを使用するかを番号Ｎ（ｋｓ）で選択する暗号鍵番号設定部１１３とのみから構成される。ここでは、データ暗号化部１１１と、暗号鍵テーブル１１２と、暗号鍵番号設定部１１３とから成る部分が、図１に示した原理図の暗号化手段１０２に相当する。

【００３３】受信装置２００は、送信装置１００の暗号鍵テーブル１１２と同じ内容を有する暗号鍵テーブル２１２と、伝送路３００を介して伝送されてきた暗号化データを暗号鍵ｋｓにより復号化するデータ復号化部２１３とを有し、これらは図１に示した原理図の復号化手段２０１に相当する。受信装置２００はさらに、データ復号化部２１３にて復号されたデータの中から誤り検出符号を検出してどのビットが誤っているかを検出する誤り検出部２１４と、この誤り検出部２１４にて一定時間内に検出された誤りの数に応じて、復号に使用している暗号鍵を変更させる暗号鍵判定部２３５とを有している。誤り検出部２１４は、図１の付帯データ検出手段２０２に相当し、暗号鍵判定部２３５は暗号鍵判定手段２０３に相当する。

【００３４】この実施例によれば、受信装置２００にてデータの誤りを検出し、検出した誤り検出情報ＥＲＲから誤り率を暗号鍵判定部２３５にて計算し、その誤り率が設定された値以下のときには復号化に使用している暗号鍵を、送信装置１００で使用している暗号鍵とすることにしている。逆に、誤り率が設定された値を越えた場合には、暗号鍵が変更されていると認識して、暗号鍵の変更を行う。この暗号鍵番号の変更は、誤り検出部２１４での誤りがなくなるか予め設定した誤り率以下になるまで繰り返して行われる。このように、暗号鍵番号を順次変更していって、誤り率が設定値より低くなると、その暗号鍵番号に相当する暗号鍵が、送信装置１００のデータ暗号化部１１１で使用した暗号鍵であると判定する。

【００３５】図８は第３実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。この図によれば、伝送路３００に送出されるデータは、送信装置１００に入力されたデータＤに誤り検出符号化部１１０にてチェックビットＣＨＫが付加されて誤り検出符号化され、さらにこの符号化されたデータが暗号化されている。この暗号化されたデータにはフレーム同期信号Ｆが付加されている。送信装置１００の暗号鍵番号設定部１１３により暗号鍵番号が変更されたとしても、変更された暗号鍵を受信側に送出することはない。

【００３６】図９は本発明の暗号化通信システムの第４実施例を示す構成図である。この実施例は第３実施例と比較して、誤り検出符号を使用する代わりにユニークワードを使用している点が相違する。

【００３７】すなわち、送信装置１００は、入力データを受けてこの入力データにユニークワードを付加するユニークワード付加部１２０を有しており、これ以外は第３実施例の構成と同じであって、データ暗号化部１１１と、暗号鍵テーブル１１２と、暗号鍵番号設定部１１３とを有している。

【００３８】一方、受信装置２００では、送信装置１００の暗号鍵テーブル１１２と同じ内容を有する暗号鍵テーブル２１２と、データ復号化部２１３とが第３実施例の構成と同じであり、これに、ユニークワード検出部２２４及び暗号鍵判定部２４５が備えられている。

【００３９】この実施例によれば、受信装置２００のユニークワード検出部２２４において、ユニークワードが検出されなければ、データ復号化部２１３での暗号鍵が間違っていると認識し、暗号鍵を変更して、ユニークワードが検出される暗号鍵を検索する。ユニークワードが検出されると、その暗号鍵は正しい暗号鍵であると判定され、その暗号鍵によるデータ復号化を行う。

【００４０】図１０は第４実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。この図によれば、伝送路３００に送出されるデータは、ユニークワード付加部１２０にて送信装置１００に入力されたデータＤの先頭にユニークワードＵＷが付加され、この付加されたデータが暗号化されている。この暗号化されたデータにはフレーム同期信号Ｆが付加されている。送信装置１００から送出されるデータには、暗号鍵番号が変

更された場合にも、暗号鍵番号の情報はない。

【００４１】図１１は本発明の暗号化通信システムの第５実施例を示す構成図である。この実施例は図７の実施例の受信装置の別な構成例として示す。受信装置２００は、図７の実施例の構成、すなわち、暗号鍵テーブル２１２と、データ復号化部２１３と、誤り検出部２１４と、暗号鍵判定部２３５とからなる構成に加え、伝送路３００からの受信データを受けて蓄積する受信バッファ部２５０と、データ復号化部２１３によって復号されたデータを蓄積する出力バッファ部２５１と、これら受信バッファ部２５０及び出力バッファ部２５１を制御するバッファ制御部２５２と、出力インタフェース部２５３とを備えている。受信バッファ部２５０は、誤り率の計算のため、暗号化データを複数フレームにわたって連続して蓄積することができ、しかも少なくとも暗号鍵を全部切り替えて誤りをチェックしている間に受信されるデータ容量分の容量を有している。

【００４２】ここで、暗号鍵が合っている場合の作用について説明する。受信データは、最初、受信バッファ部２５０にて蓄積される。次いで、バッファ制御部２５２は受信バッファ部２５０に対して蓄積されているデータをデータ復号化部２１３に転送するよう指示する。転送されたデータは、データ復号化部２１３において暗号鍵ｋｓによる復号化が行われる。復号されたデータは出力バッファ部２５１に蓄積されるとともに、誤り検出部２１４にてデータの誤り検出が行われる。暗号鍵が送信側と合っていれば、復号されたデータには殆ど誤りは含まれていないので、誤り検出部２１４で検出される誤り検出情報ＥＲＲは少なく、暗号鍵判定部２３５では低い誤り率が計算される。このとき、暗号鍵判定部２３５は、暗号鍵は正しいと判定し、その判定結果Ａ（ｋｓ）をバッファ制御部２５２に通知する。バッファ制御部２５２は、暗号鍵が正しいという判定結果Ａ（ｋｓ）を受けると、出力バッファ部２５１に対して出力許可信号を送り、出力バッファ部２５１に蓄積されているデータを出力インタフェース部２５３に送出させるとともに、受信バッファ部２５０に対して該当するデータを削除する削除信号を与えるようにする。

【００４３】次に、暗号鍵が異なっている場合の作用について説明する。バッファ制御装置２５２は、まず、受信バッファ部２５０に対して受信データをデータ復号化部２１３に転送するように指示する。データ復号化部２１３にて復号されたデータは、暗号鍵が間違っているために、多数の誤りが含まれており、出力バッファ部２５１には、誤りが含まれた状態で蓄積される。誤り検出部２１４では誤りを検出し、誤り検出情報ＥＲＲを暗号鍵判定部２３５に送出する。暗号鍵判定部２３５は、高い誤り率を認識して暗号鍵が誤っていると判定する。暗号鍵判定部２３５は、暗号鍵テーブル２１２に対して現在使用している暗号鍵番号と異なる暗号鍵番号を通知するとともに、暗号鍵が誤っているとの判定結果Ａ（ｋｓ）をバッファ制御部２５２に通知する。暗号鍵テーブル２１２は、通知された新しい暗号鍵番号Ｎ（ｋｓ）に対応する暗号鍵ｋｓをデータ復号化部２１３に設定する。バッファ制御部２５２では、受信バッファ部２５０に対して前回復号化が試みられたデータのデータ復号化部２１３への再転送を要求する。

【００４４】データ復号化部２１３は、再転送されたデータに対して新しい暗号鍵による復号を行い、出力バッファ部２５１に渡される。出力バッファ部２５１では、先に蓄積されていたデータを追い出しながら又は予め削除して、今回復号されたデータを蓄積する。この復号されたデータに誤りが含まれていなければ、新たに設定した暗号鍵が正しい暗号鍵であると判定され、バッファ制御部２５２は、出力バッファ部２５１に対して蓄積データを出力インタフェース部２５３に送出させるとともに、受信バッファ部２５０に対して該当するデータを削除するようにする。もし、今回の暗号鍵を使用した復号化でも、データの誤り率が高い場合には、再度、暗号鍵を変更するようにし、暗号鍵が正しいと判断されるまで、暗号鍵の変更を続ける。

【００４５】この構成によれば、受信データを一度蓄積しておき、正しい暗号鍵による復号化ができなければ、正しい暗号鍵が検出されるまで蓄積されているデータについて繰り返し復号化を試みることができるので、送信されたデータは途中で欠落することなくすべて正しく受信することができる。

【００４６】なお、この受信バッファ部２５０と、出力バッファ部２５１と、バッファ制御部２５２と、出力インタフェース部２５３とを追加する実施例は、図７の実施例の受信装置への適用に限定されるものではなく、図２、図５及び図９の実施例の受信装置にも同様に適用することができる。

【００４７】図１２は本発明の暗号化通信システムをディジタル画像放送に適用した構成例を示す図である。この図において、送信局５００は、ビデオテープレコーダなどのアナログ映像信号を再生する画像再生装置５１０と、アナログ映像信号をディジタル化して圧縮するディジタル画像圧縮装置５２０と、送信側暗号装置５３０と、暗号鍵選択装置５４０と、変調装置５５０と、無線送信機５６０とにより構成されている。暗号鍵選択装置５４０は、送信側暗号装置５３０に含まれる暗号鍵番号設定部の一部を構成するもので、暗号鍵番号変更時の操作が容易なように、その選択操作部のみを送信側暗号装置５３０から切り離して、たとえば、画像再生装置５１０の近くに設置される。そして、無線送信機５６０の出力は、送信アンテナ６１０に接続されている。

【００４８】受信局７００は、受信アンテナ６２０の出力を受けるチューナ７１０と、受信側暗号装置７２０と、圧縮されたディジタル映像データを伸張してアナロ

グ映像信号に変換するディジタル画像伸張装置７３０と、画像表示用ディスプレイ７４０とによって構成されている。

【００４９】ここで、送信側暗号装置５３０がディジタル映像データに対して誤り検出符号化を行い、かつ受信側に暗号鍵番号を通知しないタイプの暗号装置であり、暗号鍵が暗号鍵選択装置５４０により変更された場合のこのディジタル画像放送システムの作用について説明する。

【００５０】送信局５００において、暗号鍵選択装置５４０からの暗号鍵変更指示を受けた送信側暗号装置５３０は、指示された暗号鍵を暗号鍵テーブルより読みだし、データ暗号化部へセットする。画像再生装置５１０より出力されるアナログ信号は、ディジタル画像圧縮装置５２０にてディジタルデータに変換され、送信側暗号装置５３０に入力される。送信側暗号装置５３０では、入力データの誤り検出符号化を行い、セットされた暗号鍵にて暗号化を行う。暗号化されたデータは変調装置５５０及び無線送信機５６０にて無線出力信号に変換され、送信アンテナ６１０より送出される。

【００５１】受信局７００においては、受信アンテナ６２０にて受信した信号は、チューナ７１０にて変換・復調されて受信側暗号装置７２０に入力される。受信側暗号装置７２０では、入力されたデータを変更前の暗号鍵がセットされたデータ復号部にて復号し、その後、誤り検出を行う。データ復号の際に、データ復号部は送信側で暗号化を行った暗号鍵とは異なった暗号鍵を使用しているので、誤り検出部ではデータの誤りが検出される。ここで検出された誤りが一定の誤り率を越えると、暗号鍵異常と判断し、予め用意してある暗号鍵をデータ復号部へ順にセットしていく。誤り率が一定値以下となると、そのときの暗号鍵が変更後の暗号鍵であると判断され、これ以降はその変更後の暗号鍵で正しく復号を行うことができるようになる。復号されたデータは、ディジタル画像伸張装置７３０にて伸張されてアナログ映像信号に変換され、最終的に画像表示用ディスプレイ７４０に表示される。

【００５２】図１３はディジタル画像放送システムの各部でのデータイメージを示す図である。図において、アナログ映像信号は、送信局５００の画像再生装置５１０から出力された信号をイメージしている。ディジタル圧縮映像データは、ディジタル画像圧縮装置５２０によってディジタル化されて圧縮された画像データであり、各画像データの先頭にはフレーム同期信号Ｆが挿入されている。暗号化データは、送信側暗号装置５３０の出力信号であり、各画像データは誤り検出符号のチェックビットＣＨＫとともに暗号化されている。次の無線電波は、送信アンテナ６１０より空中に放射されて受信アンテナ６２０にて受信されるまでの信号を示している。受信データはチューナ７１０の出力における復調データであり、空中の伝送路に誤りがなければ、暗号化データと同じ信号となる。その下のディジタル圧縮映像データは、受信側暗号装置７２０にてデータ復号された信号であり、画像データが圧縮された状態のディジタル信号である。アナログ映像信号は、圧縮された画像データがディジタル画像伸張装置７３０にて元に戻され、さらにアナログ信号に変換されて画像表示用ディスプレイ７４０に入力される信号を示している。

【００５３】図１４はディジタル画像放送システムの送信側暗号装置の構成例を示す図である。この図において、送信側暗号装置５３０は、暗号鍵選択装置５４０から暗号鍵変更指示が入力される暗号鍵番号設定部５３１と、複数の暗号鍵を暗号鍵番号と対応させて格納してあるＲＯＭ化された暗号鍵テーブル５３２と、ディジタル画像圧縮装置５２０からの送信データにパリティ符号を付加する誤り検出符号化部５３３と、暗号鍵番号設定部５３１にて設定された暗号鍵番号に対応する暗号鍵によってパリティ符号が付加された送信データを暗号化する、たとえばＤＥＳ符号化ＬＳＩとするデータ暗号化部５３４とで構成される。暗号鍵番号設定部５３１はさらに、外部インタフェース回路５３１１と暗号鍵ラッチ回路５３１２とで構成されている。

【００５４】暗号鍵選択装置５４０から暗号鍵変更指示が送信側暗号装置５３０の暗号鍵設定部５３１に入ると、その指示は暗号鍵番号設定部５３１の外部インタフェース回路５３１１を介して暗号鍵ラッチ回路５３１２に入力され、ここでラッチされる。これにより、暗号鍵が送信側暗号装置５３０に設定されることになる。ラッチされた暗号鍵番号から暗号鍵テーブル５３２を使って暗号鍵が選び出される。次に、誤り検出符号化部５３３にて送信データに誤り検出符号化したものをデータ符号化部５３４に入れ、選び出された暗号鍵を使って暗号化する。暗号化されたデータは、変調装置５５０への送出信号となる。

【００５５】図１５はディジタル画像放送システムの受信側暗号装置の構成例を示す図である。この図において、受信側暗号装置７２０は、チューナ７１０からの受信信号を受ける、たとえばＤＥＳ復号化ＬＳＩとするデータ復号部７２１と、パリティチェック回路を構成する誤り検出部７２２と、暗号鍵判定部７２３と、送信側暗号装置５３０の暗号鍵鍵テーブル５３２と同じＲＯＭ化された暗号鍵鍵テーブル７２４とで構成される。暗号鍵判定部７２３としては、誤り検出部７２２からの誤り情報を受けて誤り数を数える誤り数カウンタ回路７２３１と、たとえば１分間当たりの誤り数から誤り率を計算する時間保護回路７２３２と、計算された誤り率に応じて暗号鍵番号を順次変更する鍵番号カウンタ回路７２３３とから構成されている。

【００５６】受信信号を受けたデータ復号化部７２１は暗号鍵テーブル７２４から与えられていた暗号鍵によっ

て復号する。このとき、その暗号鍵が合っていれば、受信信号は正しく復号され、暗号鍵が違っていれば、無効なデータに変換される。復号化されたデータは、誤り検出部７２２にてパリティチェックを受け、チェックビットを除いた画像データが受信データとしてディジタル画像伸張装置７３０に送出される。パリティチェックによって誤りが検出されれば、誤り検出部７２２は、誤り情報を暗号鍵判定部７２３に送り出す。この誤り情報は誤り数カウンタ回路７２３１にてカウントされ、時間保護回路７２３２にて誤り率が計算される。この誤り率が所定値以上になると鍵番号カウンタ回路のカウンタ値を１つずつ増加させて、暗号鍵番号を順次変更する。したがって、次の受信信号に対しては、この変更された暗号鍵番号に対応する暗号鍵によって復号化することになる。

【００５７】

【発明の効果】以上説明したように本発明では、送信側において、暗号化すべきデータに何らかの付帯データを付加し、受信側では復号した後のデータからその付帯データを検出するようにし、そして、その付帯データが正常に検出できなければ、受信側の暗号鍵を順次変えていくように構成した。このため、使用する暗号鍵を変更したときに、送信側から使用した暗号鍵の番号が受信側に正常に通知できなかった場合にも、受信側のみで回復することができる。

【００５８】また、受信側に積極的に暗号鍵の番号を伝送しなくても、受信側で暗号鍵の変更をすることができるので、暗号化データ通信システムの信頼性及び秘匿強度を強化することができる。

【００５９】さらに、バッファ手段を使用して、正しい暗号鍵による正常な復号が行われたときのみ、復号化データを出力することにより、送信されたデータは欠落なくすべて正しく受信することができる。

【図面の簡単な説明】

【図１】本発明の原理を示す構成図である。

【図２】本発明の暗号化通信システムの第１実施例を示す構成図である。

【図３】暗号鍵判定部の一例を示す構成図である。

【図４】第１実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。

【図５】本発明の暗号化通信システムの第２実施例を示す構成図である。

【図６】第２実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。

【図７】本発明の暗号化通信システムの第３実施例を示す構成図である。

【図８】第３実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。

【図９】本発明の暗号化通信システムの第４実施例を示す構成図である。

【図１０】第４実施例の暗号化通信システムの伝送路上のデータイメージを示す図である。

【図１１】本発明の暗号化通信システムの第５実施例を示す構成図である。

【図１２】本発明の暗号化通信システムをディジタル画像放送に適用した構成例を示す図である。

【図１３】ディジタル画像放送システムの各部でのデータイメージを示す図である。

【図１４】ディジタル画像放送システムの送信側暗号装置の構成例を示す図である。

【図１５】ディジタル画像放送システムの受信側暗号装置の構成例を示す図である。

【図１６】従来の暗号化通信システムの構成を示す図である。

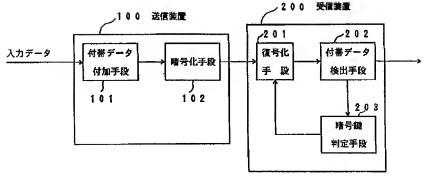
【図１７】従来の暗号化通信システムの伝送路上のデータイメージを示す図である。

【符号の説明】

１００　送信装置
１０１　付帯データ付加手段
１０２　暗号化手段
１１０　誤り検出符号化部
１２０　ユニークワード付加部
２００　受信装置
２０１　復号化手段
２０２　付帯データ検出手段
２０３　暗号鍵判定手段
２１４　誤り検出部
２１５　暗号鍵判定部
２２４　ユニークワード検出部
２２５　暗号鍵判定部

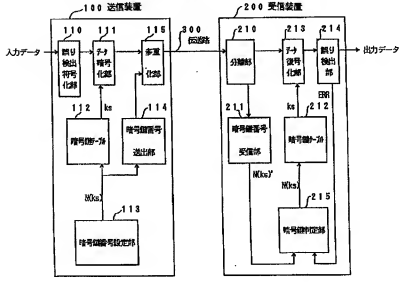
【図1】

本発明の原理を示す構成図



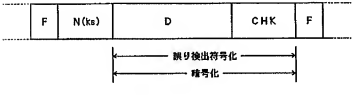

【図2】

本発明の暗号化通信システムの第1実施例を示す構成図



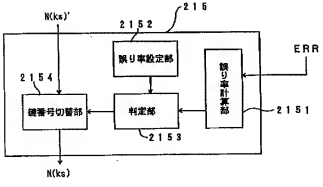

【図4】

第1実施例の暗号化通信システムの伝送路上のデータイメージを示す図



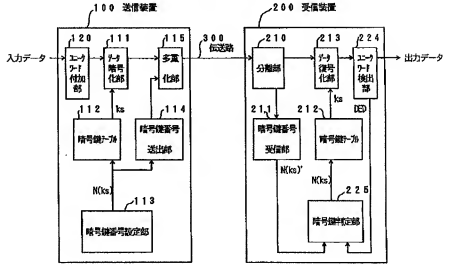
【図3】

暗号鍵判定部の一例を示す構成図



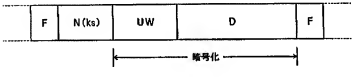

【図5】

本発明の暗号化通信システムの第2実施例を示す構成図



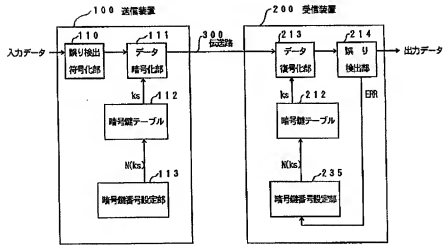

【図6】

第2実施例の暗号化通信システムの伝送路上のデータイメージを示す図



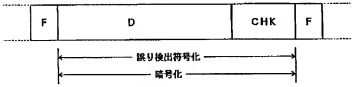
【図7】

本発明の暗号化通信システムの第3実施例を示す構成図



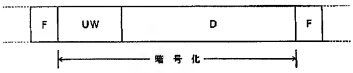

【図8】

第3実施例の暗号化通信システムの伝送路上のデータイメージを示す図



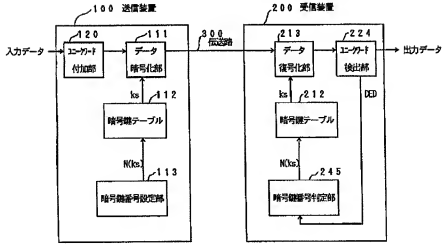

【図10】

第4実施例の暗号化通信システムの伝送路上のデータイメージを示す図



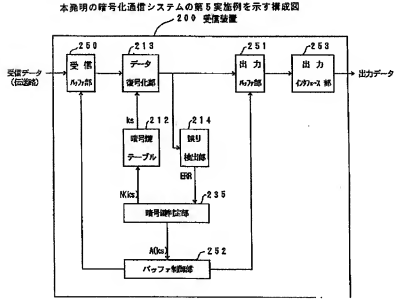
【図９】

本発明の暗号化通信システムの第４実施例を示す構成図



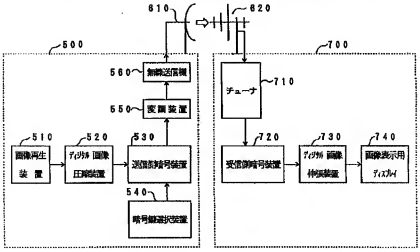

【図１１】

本発明の暗号化通信システムの第５実施例を示す構成図



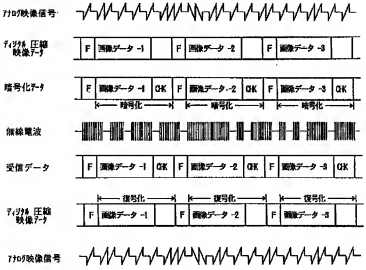
【図１２】

本発明の暗号化通信システムをディジタル画像放送に適用した構成例を示す図



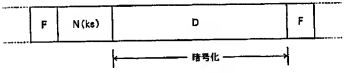

【図１３】

ディジタル画像放送システムの各部でのデータイメージを示す図



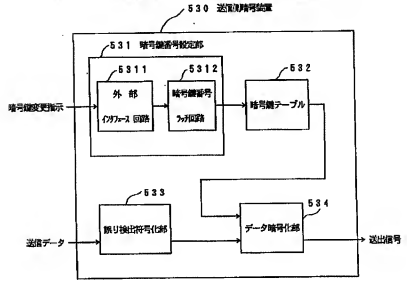

【図１７】

従来の暗号化通信システムの伝送路上のデータイメージを示す図



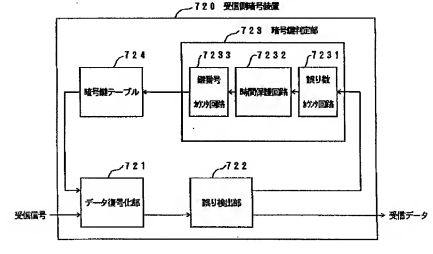
【図１４】

ディジタル画像放送システムの送信側暗号装置の構成例を示す図



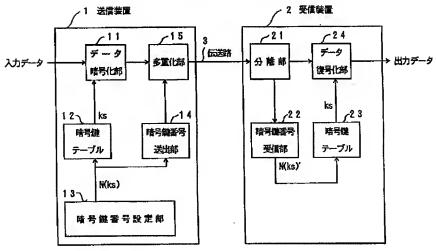

【図１５】

ディジタル画像放送システムの受信側暗号装置の構成例を示す図



【図16】

従来の暗号化通信システムの構成を示す図



# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-327029
(43)Date of publication of application : 12.12.1995

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 06-117828
(22)Date of filing : 31.05.1994

(71)Applicant : FUJITSU LTD
(72)Inventor : UENO TOMOYUKI
SETA MITSURU

## (54) CIPHERING COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To correct a ciphering key number at a receiver side even when the ciphering key number is not correctly reported to the receiver side with respect to the ciphering communication system having plural ciphering keys used to cipher data and using one of them switchingly at any time.
CONSTITUTION: A transmitter 100 is provided with additional data addition means 101 adding any additional data to data to be cipheredand a receiver 200 is provided with an additional data detection means 202 detecting the additional data from the data after decoding and a ciphering key discrimination means 203 revising sequentially the ciphering key of the receiver 200 when the additional data cannot normally be detected. Thuseven when the number of a ciphering key is not normally reported on the revision of a ciphering keyit is recovered by the receiver side only.

## CLAIMS

[Claim(s)]
[Claim 1]An encryption communication system with two or more encryption keys used if needed of being characterized by comprising the following changing at any time.
A sending set (100) provided with an encoding means (102) which enciphers to said input data and incidental data which have an incidental data addition means (101) which adds incidental data to input data which should be encipheredand two or more encryption keys used changingand are outputted from said incidental data addition means.
A decoding means (201) which decodes encryption data received via a

transmission lineAn incidental data detection means (202) to detect incidental data added to input dataAnd a receiving set (200) provided with an encryption key judging means (203) it is directed that changes an encryption key used for decryption to said decoding means when it judges whether an encryption key used for decryption according to an error rate of detected incidental data is the right and judges with said encryption key not being right.

[Claim 2]Said encoding means (102) equips a means to encipher said input data and incidental data from said incidental data addition means according to a set-up encryption keyand enciphered data with a means to multiplex a number of an encryption key used for encryptionSaid decoding means (201) acquires a number of an encryption key which separates a number of an encryption key from received dataand is used for decodingThe encryption communication system according to claim 1 provided with a means to answer a decision result that an encryption key is not right from said encryption key judging meansand to change a number of said encryption key.

[Claim 3]Said incidental data addition means (101) is made into an error detecting code-ized part which codes input data with an error detecting codeThe encryption communication system according to claim 1 making said incidental data detection means (202) into an error detection part which inspects an error detecting code decrypted by said decoding means.

[Claim 4]Said incidental data addition means (101) is made into a unique word adjunct which adds unique word to input dataThe encryption communication system according to claim 1 making said incidental data detection means (202) into a unique-word-detection part which inspects unique word decrypted by said decoding means.

[Claim 5]A receiving set of an encryption communication system with two or more encryption keys used if needed of being characterized by comprising the following changing at any time.

A decoding means (201) which decodes encryption data received via a transmission line with an encryption key set up beforehand.

An incidental data detection means (202) to detect incidental data added to input data from decrypted dataAn encryption key judging means (203) which judges whether an encryption key used for decryption according to an error rate of detected incidental data is the rightand makes an encryption key of said decoding means change when an encryption key is not right.

[Claim 6]The receiving set comprising according to claim 5:

A data decryption-ized part decrypted with an encryption key which said decoding means (201) inputted encryption data transmitted via a transmission lineand was specified.

A cryptograph key table which has the same contents as a cryptograph key table of a sending set.

[Claim 7]The receiving set according to claim 6wherein said decoding means (201)

is further provided with a separation part which inputs encryption data transmitted via a transmission lineand separates an encryption key number from encryption dataand an encryption key number receive section which receives a separated encryption key number.

[Claim 8]The receiving set according to claim 5wherein said incidental data detection means (202) is an error detection part which inspects an error detecting code decrypted by said decoding means.

[Claim 9]The receiving set according to claim 5wherein said encryption key judging means (203) is an encryption key judgment part which makes an encryption key used for decoding according to an error rate detected in said error detection part change.

[Claim 10]An error rate calculating means which computes an error rate based on information which said encryption key judgment part detected by said incidental data detection meansThe receiving set according to claim 9 comprising a judging means judge that is [ an encryption key used for decryption ] unusual when a computed error rate exceeds a predetermined valueand a key number switching means which changes an encryption key number prepared when it judged that an encryption key is unusual one by one. [ two or more ]

[Claim 11]The receiving set according to claim 5 being a unique-word-detection part which inspects unique word decrypted by said incidental data detection means (202) and ****** decoding means.

[Claim 12]The receiving set according to claim 5wherein said encryption key judging means (203) is an encryption key judgment part which makes an encryption key used for decoding according to a non-detection ratio of unique word detected in said unique-word-detection part change.

[Claim 13]A receive buffer means to store received encryption dataand an output buffer means which stores data decrypted by said decoding meansDirections which delete data decrypted [ the ] when data decoded while directing transmission of received data to said decoding means for said receive buffer means is normal are issuedThe receiving set according to claim 5 having further a buffer control means which issues directions which output the data as valid data when data decoded by said output buffer means is normal.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application]Especially this invention has two or more encryption keys used in order to encipher data about an encryption communication systemand relates to the encryption communication system in a data communication system which changes and uses these encryption keys if needed.

[0002]Even if the data which transmits a communication line top is monitored conventionallyin order to keep the contents which the data means from being

understoodthe method of enciphering the required data of security protection and transmitting is taken. In a cipher systemDES (Data Encryption Standard)There is the method of using secretssuch as FEAL (Fast data Encipherment ALgorithm)and an open encryption keyand normal data communications are performed using the same encryption key by the transmitting side and a receiver.

[0003]

[Description of the Prior Art]Drawing 16 is a figure showing the composition of the conventional encryption communication system. In a figurethe conventional encryption communication system comprises the receiving set 2 for decoding in response to the sending set 1 and its encryption data for enciphering and sending data. Although the transmission line 3 between the sending set 1 and the receiving set 2 does not carry out regulation in particularit is what takes the gestalt of a cable like a telephone wirefor exampleor takes the gestalt of radio like communication using a satellite. The sending set 1 and the receiving set 2 of the graphic display are shown only about the portion concerning encryption.

[0004]The data encryption part 11 as which the sending set 1 enciphers input data with the encryption key ksThe cryptograph key table 12 changed into the encryption key ks from specified number N (ks)The encryption key number set part 13 which chooses whether the encryption key ks of cryptograph key table 12 throat is used in order to encipher input data by the number N (ks)It comprises the encryption key number sending part 14 for sending the encryption key number N (ks) selected by the encryption key number set part 13 to the receiving set 2and the enciphered data and the multiplexing part 15 which multiplexes the encryption key number N (ks).

[0005]The separation part 21 which the receiving set 2on the other handinputs the encryption data transmitted via the transmission line 3and is divided into encryption data and an encryption key numberIt comprises the encryption key number receive section 22 which receives the separated encryption key numberthe cryptograph key table 12 of the sending set 1 and the cryptograph key table 23 which has the same contentsand the data decryption-ized part 24 which decrypts the separated encryption data with the encryption key ks specified by encryption key number N(ks)'.

[0006]The sending set 1 and the receiving set 2 have the same cryptograph key tables 12 and 23 that have two or more encryption keysTo the receiving set 2only the encryption key number corresponding to the encryption key used for the data encryption to transmit is transmittedand it is decodedand he acquires an encryption key numberand is trying to decode in a receiver the data which took out the same encryption key as the transmitting side from this encryption key numberand was enciphered. According to this compositionsince an encryption key number can be changed at any time and the encryption key itself is not transmittedthe high transmission line of privacy is secured.

[0007]Drawing 17 is a figure showing the data image on the transmission line of the conventional encryption communication system. According to this figurethe data on the transmission line 3 sent out from the sending set 1 comprises D

enciphered by the data encryption part 11and encryption key number N (ks) which it was outputted from the encryption key number sending part 14and was multiplexed by the multiplexing part 15 and frame alignment signal F. The encryption key number N (ks) may usually always send for every constant period or every frame only at the time of a data-communications startalthough it is made to be sent only at the time of the change.

[0008]

[Problem(s) to be Solved by the Invention]Howeverin the conventional encryption communication system with two or more encryption keys. Since he is trying to send the information on an encryption key number from a sending set to a receiving setFor examplewhen one information about the encryption key number has been mistaken by chance among the data sent out at the time of an encryption key changed numberin order to decode with the encryption key corresponding to the encryption key number notified previouslyeven all other data is mistaken and right decoding becomes impossible. And all the received data becomes unusual until an encryption key number is notified correctly in such a case.

[0009]If it is detected that encryption keys differ if it is a both directions type communications systemcan also require resending of an encryption key numberbut. All received data become unusual until an encryption key number is notified correctlysince request sending is impossible in the case of uni-directional formal ** systemssuch as broadcast.

[0010]This invention is made in view of such a pointand is a thing.

In a case so that the purpose may be used and an encryption key number may be transmitted only at an interval like [ at the time of encryption key change ]even if an encryption key number is notified accidentallyit is providing the encryption communication system corrected for a right encryption key number.

[0011]Even if it does not send the encryption key number itselfthis invention finds out the same encryption key number as the transmitting side by a receiverand an object of this invention is to provide the encryption communication system which follows in footsteps of it and is corrected for the same encryption key number as the transmitting side also when there is change to an encryption key.

[0012]Furthermoreall the data in which this invention was transmitted aims at providing an encryption communication system receivable without an error.

[0013]

[Means for Solving the Problem]Drawing 1 is a lineblock diagram showing a principle of this invention which attains the above-mentioned purpose. The incidental data addition means 101 which adds incidental data to input data which should encipher the sending set 100 in this figureIt has two or more encryption keys used changingand comprises the encoding means 102 which enciphers to input data and incidental data which are outputted from the incidental data addition means 101. The decoding means 201 whichon the other handdecodes encryption data in which the receiving set 200 was received via a transmission

lineIt comprises the incidental data detection means 202 to detect incidental data added to input dataand the encryption key judging means 203 it is directed to the decoding means 201 that change an encryption key used for decryption according to an error rate of detected incidental data.

[0014]

[Function]According to the above-mentioned meansin the sending set 100after adding the incidental data which can be identified when an error is generated in a transmission line to the input data which should be encipheredthese data is enciphered by the encoding means 102. The encoding means 102 is provided with the table with two or more encryption keys.

The encryption key used for encryption if needed is changed at any time.

In the receiving set 200received data are decrypted by the decoding means 201and incidental data is further detected from the decrypted data by the incidental data detection means 202. If the encryption key judging means 203 calculates the error rate of the detected incidental data firstit judges with it being the error produced in the transmission line when there are few the error ratesand an error rate exceeds a predetermined valueIt directs to use the encryption key which judges with having mistaken the encryption key currently used by the decoding means 201and is different to the decoding means 201.

[0015]

[Example]Firstthe outline of the example of this invention is explained. Drawing 1 is a lineblock diagram showing the principle of this invention. According to the encryption communication system of this inventionthe sending set 100The incidental data addition means 101 which adds incidental data to the input data which should be encipheredComprise the encoding means 102 which enciphers to the input data and incidental data which are outputted from the incidental data addition means 101and the receiving set 200The decoding means 201 which decodes the encryption data received via the transmission lineIt comprises the incidental data detection means 202 to detect the incidental data added to input dataand the encryption key judging means 203 it is directed to the decoding means 201 that change the encryption key used for decryption according to the error rate of the detected incidental data.

[0016]Firstin the sending set 100after adding the incidental data which can be identified when an error is generated in a transmission line to the input data which should be encipheredthese data is enciphered by the encoding means 102. The encoding means 102 is provided with the table with two or more encryption keys.

The encryption key used for encryption if needed is changed at any time.

In the receiving set 200received data are decrypted by the decoding means 201and incidental data is further detected from the decrypted data by the incidental data detection means 202. If the encryption key judging means 203 calculates the error rate of the detected incidental data firstit judges with it being the error produced in the transmission line when there are few the error ratesand an error rate exceeds a predetermined valueIt directs to use the encryption key which judges with having mistaken the encryption key currently used by the

decoding means 201and is different to the decoding means 201. By thisin the receiving set sideselection use of the right encryption key will always be carried out.

[0017]Drawing 2 is a lineblock diagram showing the 1st example of the encryption communication system of this invention. In this figurethe encryption communication system of this invention comprises the sending set 100the receiving set 200and the transmission line 300 made into the communication line between these.

[0018]The sending set 100 has the error detecting code-ized part 110 which codes and adds an error detecting code to this input data in response to input data. This error detecting code-ized part 110 is equivalent to the incidental data addition means 101 of a principle figure shown in drawing 1and as an error detecting codeFor exampleerror detection correction codessuch as parity check numeralsBCH (Bose-Chaudhuri-Hocquenghem) numeralsand a convolutional codeare used. The data encryption part 111 as which the sending set 100 enciphers input data with the encryption key ks furtherThe cryptograph key table 112 changed into the encryption key ks from specified number N (ks)The encryption key number set part 113 which chooses whether the encryption key ks of cryptograph key table 112 throat is used in order to encipher input data by the number N (ks)The encryption key number sending part 114 for notifying the encryption key number N (ks) selected by the encryption key number set part 113 to the receiving set 200It has the enciphered data and the multiplexing part 115 which multiplexes the encryption key number N (ks)and these composition is equivalent to the encoding means 102 of a principle figure shown in drawing 1.

[0019]The separation part 210 which the receiving set 200 inputs the encryption data transmitted via the transmission line 300and is divided into encryption data and an encryption key numberIt has the data decryption-ized part 213 decrypted with the encryption key number receive section 211 which receives the separated encryption key numberthe cryptograph key table 112 of the sending set 100 and the cryptograph key table 212 which has the same contentsand the encryption key ks which had the separated encryption data specified. These composition is equivalent to the decoding means 201 of a principle figure shown in drawing 1. The error detection part 214 which detects which bit the receiving set 200 detected the error detecting code further out of the data decoded in the data decryption-ized part 213and has mistaken itAccording to the number of the errors detected in fixed time by this error detection part 214i.e.an error rateit has the encryption key judgment part 215 which makes the encryption key currently used for decoding change. The error detection part 214 is equivalent to the incidental data detection means 202 of drawing 1and the encryption key judgment part 215 is equivalent to the encryption key judging means 203.

[0020]Thustwo or more encryption keys are beforehand prepared for the sending set 100 and the receiving set 200an encryption key number is given to them to each encryption keyand it is putting into the cryptograph key tables 112 and 212 which are those conversion tables. In changing an encryption keyit chooses the

one encryption key ks by the encryption key number N (ks) by the encryption key number set part 113 of the sending set 100 from the encryption keys currently prepared beforehand. The selected encryption key number N (ks) is changed into the encryption key number ks with the cryptograph key table 112and it is notified to a receiver via the encryption key number sending part 114 and the multiplexing part 115 while being used in the data encryption part 111. To input dataan error detecting code is added in the error detecting code-ized part 110and it is enciphered in the data encryption part 111.

[0021]In the receiving set 200by the separation part 210the multiplexed encryption key number is separated and it is received in the encryption key number receive section 211. Since the received encryption key number may be mistaken in the transmission line 300N(ks)' has shown it. Noting that encryption key number N(ks)' first received in the encryption key judgment part 215 is right encryption key number N (ks)The encryption key ks which the cryptograph key table 212 is referred by that encryption key number N (ks)and corresponds is chosenand decoding by this encryption key ks is performed in the data decryption-ized part 213. In the error detection part 214it is detected whether the error detecting code-ized data decrypted in the data decryption-ized part 213 using the error detecting code has an error. If an error is detectedthe error detection part 214 will output error detection information ERR. In the encryption key judgment part 215error detection information ERR from the error detection part 214 is receivedIt judges whether it is what was produced when the encryption key had mistaken whether it is what the information produced accidentally in the transmission line 300and when [ which an error rate is high and the encryption key has mistaken ] it seems that it isan encryption key number is changed and decryption is tried using the encryption key corresponding to the encryption key number. Change of this encryption key number is repeated until it becomes whether the error in the error detection part 214 is lostand below the error rate defined beforehand.

[0022]Drawing 3 is a lineblock diagram showing an example of an encryption key judgment part. The error rate calculation part 2151 in which the encryption key judgment part 215 receives error detection information ERR from the error detection part 214 in this figureWhen encryption key number N(ks)' which received in the error rate set part 2152the judgment part 2153and the encryption key number receive section 211 is receivedit comprises the key number switching part 2154 which holds this and is given to the cryptograph key table 212 as encryption key number N (ks).

[0023]The error rate calculation part 2151 calculates an error rate in response to error detection information ERR from the error detection part 214. The judgment part 2153 compares the error rate calculated by the error rate calculation part 2151 with the error rate set up by the error rate set part 2152When an error rate is lowit judges with the transmission error having occurred on the transmission line 300and if higher than the error rate to which the error rate was setit will judge with the encryption key currently used in the data decryption-ized part 213 being wrong. When judged with the encryption key being wrongthe key number switching

part 2154 changes the encryption key number corresponding to encryption key number N(ks)' which received in the encryption key number receive section 211 to another encryption key number. For examplesupposing it is outputting encryption key number N(ks) =1 in response to the input of encryption key number N(ks)'encryption key number N(ks) =2 will be outputted. This change is performed one by one within the limits of the encryption key number corresponding to two or more encryption keys prepared beforehandand it is repeated until an error rate reaches below the value set up by the error rate set part 2152.

[0024]Drawing 4 is a figure showing the data image on the transmission line of the encryption communication system of the 1st example. According to this figurein the error detecting code-ized part 110the check bit CHK is added to the data D inputted into the sending set 100the data sent out to the transmission line 300 is error-detecting-code-izedand this coded data is enciphered. Frame alignment signal F is added to this enciphered data. When an encryption key number is changed by the encryption key number set part 113 of the sending set 100the encryption key number N (ks) by which the setting variation was carried out is inserted and sent to the head of the data D like a graphic display.

[0025]Drawing 5 is a lineblock diagram showing the 2nd example of the encryption communication system of this invention. The point which is using unique word is different instead of this example using an error detecting code as compared with the 1st example.

[0026]That isthe sending set 100 has the unique word adjunct 120 which adds unique word to this input data in response to input data. Generallyother data is data which has a bit row of the impossible specific pattern which consists of the existing number of bits [ like ] which was decided to other data with a large differenceand moreovereven if 1 bit has mistaken unique wordIf the whole is seenit will be the word which has a value which can imagine that it is unique word.

[0027]The sending set 100 of everything but the unique word adjunct 120 is the same as that of the composition of the 1st exampleand has the data encryption part 111the cryptograph key table 112the encryption key number set part 113the encryption key number sending part 114and the multiplexing part 115.

[0028]On the other hand with the receiving set 200the separation part 210 and the encryption key number receive section 211The cryptograph key table 112 of the sending set 100the cryptograph key table 212 of the same contentsand the data decryption-ized part 213 are the same as the composition of the 1st exampleand this is equipped with the unique-word-detection part 224 and the encryption key judgment part 225.

[0029]In this examplethe coding for error detection is not performed to the whole input dataHe enciphers and sends what only added unique word to input data at the transmitting sideand is trying to judge the encryption key currently used to be the right by the unique word being correctly detected from the decrypted data in a receiver. Detection of unique word is performed in the unique-word-detection part 224 of the receiving set 200and when unique word is detectedthe unique-word-detection information DED is outputted. When unique word is not detected

correctlythe unique-word-detection information DED turns into information showing unique word un-detecting. In the encryption key judgment part 225the ratei.e.the non-detection ratio which is unique wordthat unique word is undetectable is calculated in response to the unique-word-detection information DED. If the non-detection ratio of unique word increasesthe cause will be judged to be what is not an error of the transmission line 300 and is depended on a difference of an encryption keyand will be made to change an encryption key number.

[0030]Drawing 6 is a figure showing the data image on the transmission line of the encryption communication system of the 2nd example. According to this figurethe unique word UW is simply added at the head of the data D by which the data sent out to the transmission line 300 was inputted into the sending set 100 by the unique word adjunct 120and this added data is enciphered. Frame alignment signal F is added to this enciphered data. When an encryption key number is changed by the encryption key number set part 113 of the sending set 100the changed encryption key number N (ks) of the enciphered data is inserted and sent to a head like a graphic display.

[0031]Drawing 7 is a lineblock diagram showing the 3rd example of the encryption communication system of this invention. The point which does not send out to a receiver the encryption key number as which this example was chosen by the encryption key number set part 113 as compared with the 1st example is different.

[0032]Namelythe error detecting code-ized part 110 which the sending set 100 codes an error detecting code to this input data in response to input dataand is addedThe data encryption part 111 which enciphers input data with the encryption key ksIn order to encipher input data as the cryptograph key table 112 changed into the encryption key ks from specified number N (ks)whether the encryption key ks of cryptograph key table 112 throat is used consists of only the encryption key number set parts 113 chosen by the number N (ks). Herethe portion which comprises the data encryption part 111the cryptograph key table 112and the encryption key number set part 113 is equivalent to the encoding means 102 of a principle figure shown in drawing 1.

[0033]The cryptograph key table 212 which has the contents as the cryptograph key table 112 of the sending set 100 with the same receiving set 200It has the data decryption-ized part 213 which decrypts the encryption data transmitted via the transmission line 300 with the encryption key ksand these are equivalent to the decoding means 201 of a principle figure shown in drawing 1. The error detection part 214 which detects which bit the receiving set 200 detected the error detecting code further out of the data decoded in the data decryption-ized part 213and has mistaken itAccording to the number of the errors detected in fixed time by this error detection part 214it has the encryption key judgment part 235 which makes the encryption key currently used for decoding change. The error detection part 214 is equivalent to the incidental data detection means 202 of drawing 1and the encryption key judgment part 235 is equivalent to the encryption key judging means 203.

[0034]According to this examplethe receiving set 200 detects the error of data and an error rate is calculated by the encryption key judgment part 235 from detected error detection information ERRThe encryption key currently used for decryption when it is below the value to which the error rate was set is made to consider it as the encryption key currently used with the sending set 100. On the contrarywhen the value to which the error rate was set is exceededit is recognized as the encryption key being changed and an encryption key is changed. A change of this encryption key number is repeatedly made until it becomes whether the error in the error detection part 214 is lostand below the error rate set up beforehand. Thusan encryption key number is changed one by oneand if an error rate becomes lower than a preset valueit will judge with the encryption key equivalent to the encryption key number being an encryption key used in the data encryption part 111 of the sending set 100.
[0035]Drawing 8 is a figure showing the data image on the transmission line of the encryption communication system of the 3rd example. According to this figurein the error detecting code-ized part 110the check bit CHK is added to the data D inputted into the sending set 100the data sent out to the transmission line 300 is error-detecting-code-izedand this coded data is enciphered further. Frame alignment signal F is added to this enciphered data. Even if an encryption key number is changed by the encryption key number set part 113 of the sending set 100the changed encryption key is not sent out to a receiver.
[0036]Drawing 9 is a lineblock diagram showing the 4th example of the encryption communication system of this invention. The point which is using unique word is different instead of this example using an error detecting code as compared with the 3rd example.
[0037]That isthe sending set 100 has the unique word adjunct 120 which adds unique word to this input data in response to input data.
Except thisit is the same as the composition of the 3rd exampleand has the data encryption part 111the cryptograph key table 112and the encryption key number set part 113.

[0038]On the other handin the receiving set 200the cryptograph key table 112 of the sending set 100the cryptograph key table 212 which has the same contentsand the data decryption-ized part 213 are the same as the composition of the 3rd exampleand this is equipped with the unique-word-detection part 224 and the encryption key judgment part 245.
[0039]According to this examplein the unique-word-detection part 224 of the receiving set 200if unique word is not detectedit is recognized as the encryption key in the data decryption-ized part 213 being wrongan encryption key is changedand the encryption key with which unique word is detected is searched. If unique word is detectedit will be judged with the encryption key being a right encryption keyand data decryption-ization by the encryption key will be performed.
[0040]Drawing 10 is a figure showing the data image on the transmission line of the encryption communication system of the 4th example. According to this

figurethe unique word UW is added to the head of the data D by which the data sent out to the transmission line 300 was inputted into the sending set 100 by the unique word adjunct 120and this added data is enciphered. Frame alignment signal F is added to this enciphered data. Also when an encryption key number is changedthere is no information on an encryption key number in the data sent out from the sending set 100.

[0041]Drawing 11 is a lineblock diagram showing the 5th example of the encryption communication system of this invention. This example is shown as another example of composition of the receiving set of the example of drawing 7. The composition 212 of the example of drawing 7i.e.a cryptograph key tablethe receiving set 200The receive buffer part 250 which is accumulated in response to the received data from the transmission line 300 in addition to the composition which consists of the data decryption-ized part 213the error detection part 214and the encryption key judgment part 235It has the output buffer section 251 which stores the data decoded by the data decryption-ized part 213the buffer control part 252 which controls these receive buffer part 250 and the output buffer section 251and the output interface part 253. For calculation of an error ratethe receive buffer part 250 can store encryption data continuously over a multiple frameand has the capacity for the data volume received while all changing an encryption key at least moreover and checking the error.

[0042]Herean operation when the encryption key is correct is explained. Received data are accumulated in the receive buffer part 250 at first. Subsequentlythe buffer control part 252 directs to transmit the data stored to the receive buffer part 250 to the data decryption-ized part 213. Decryption according [ the transmitted data / on the data decryption-ized part 213 and ] to the encryption key ks is performed. While the decoded data is stored in the output buffer section 251error detection of data is performed by the error detection part 214. Since an error is hardly contained in the decoded data if the encryption key suits the transmitting sidethere is little error detection information ERR detected by the error detection part 214and a low error rate is calculated in the encryption key judgment part 235. At this timethe encryption key judgment part 235 judges an encryption key to be the rightand notifies that decision result A (ks) to the buffer control part 252. If an encryption key receives the decision result A (ks) of the rightthe buffer control part 252An output enabling signal is sent to the output buffer section 251and while sending out the data stored in the output buffer section 251 to the output interface part 253the deletion signal which deletes data applicable to the receive buffer part 250 is given.

[0043]Nextan operation when encryption keys differ is explained. The buffer control device 252 directs to transmit received data to the data decryption-ized part 213 to the receive buffer part 250 first. Since the encryption key has made a mistake in the data decoded in the data decryption-ized part 213many errors are contained.

Where an error is containedit is accumulated in the output buffer section 251.

In the error detection part 214an error is detected and error detection information

ERR is sent out to the encryption key judgment part 235. It judges with the encryption key judgment part 235 having recognized the high error rateand the encryption key having mistaken it. The encryption key judgment part 235 notifies the decision result A (ks) that the encryption key is mistaken to the buffer control part 252 while notifying a different encryption key number from the encryption key number used to the cryptograph key table 212 now. The cryptograph key table 212 sets the encryption key ks corresponding to the notified new encryption key number N (ks) as the data decryption-ized part 213. The buffer control part 252 requires the re transfer to the data decryption-ized part 213 of the data in which decryption was tried last time to the receive buffer part 250.

[0044]The data decryption-ized part 213 performs decoding by a new encryption key to the data by which re transfer was carried outand is passed to the output buffer section 251. In the output buffer section 251it deletes beforehanddriving out the data stored previouslyor the data decoded this time is stored. If the error is not contained in this decoded datathe newly set-up encryption key judges that it is a right encryption keyand the buffer control part 252While sending out accumulation data to the output interface part 253 to the output buffer section 251data applicable to the receive buffer part 250 is deleted. When the decryption which uses this encryption key also has a high error rate of datait continues change of an encryption key until it changes an encryption key and an encryption key is again judged to be the right.

[0045]Since decryption can be repeatedly tried about the data stored until a right encryption key is detected if according to this composition received data are accumulated once and decryption by a right encryption key cannot be performedThe transmitted data can be received correctly altogetherwithout being missing on the way.

[0046]The example which adds this receive buffer part 250the output buffer section 251the buffer control part 252and the output interface part 253It is applicable also like the receiving set of the example of not the thing limited to application to the receiving set of the example of drawing 7 but drawing 2drawing 5and drawing 9.

[0047]Drawing 12 is a figure showing the example of composition which applied the encryption communication system of this invention to digital image broadcast. The picture reproducer 510 in which the transmitting station 500 reproduces the analog video signal of a videotape recorder etc. in this figureIt is constituted by the digital image compression equipment 520 which digitizes and compresses an analog video signalthe transmitting side cryptogram decoders 530the encryption key selecting arrangement 540the modulator 550and the radio transmitter 560. The encryption key selecting arrangement 540 constitutes a part of encryption key number set part contained in the transmitting side cryptogram decoders 530it separates only the selection operation part from the transmitting side cryptogram decoders 530 so that easily [ the operation at the time of an encryption key changed number ]for exampleit is installed near the picture reproducer 510. And the output of the radio transmitter 560 is connected to the transmission antenna

610.
[0048]The receiving station 700 is constituted by the tuner 710 which undergoes the output of the receiving antenna 620the receiver cryptogram decoders 720the digital image extending apparatus 730 which elongates the compressed digital video data and is changed into an analog video signaland the display 740 for image display.
[0049]Herethe transmitting side cryptogram decoders 530 are cryptogram decoders of the type which performs error detecting code-ization to a digital video dataand does not notify an encryption key number to a receiverand an operation of this digital image broadcasting system when an encryption key is changed by the encryption key selecting arrangement 540 is explained.
[0050]In the transmitting station 500the transmitting side cryptogram decoders 530 which received the encryption key changing instruction from the encryption key selecting arrangement 540 read the directed encryption key from a cryptograph key tableand set it to a data encryption part. The analog signal outputted from the picture reproducer 510 is changed into digital data with the digital image compression equipment 520and is inputted into the transmitting side cryptogram decoders 530. In the transmitting side cryptogram decoders 530error detecting code-ization of input data is performed and it enciphers with the set encryption key. The enciphered data is changed into a radio output signal with the modulator 550 and the radio transmitter 560and is sent out from the transmission antenna 610.
[0051]In the receiving station 700with the tuner 710it changes and gets over and the signal received with the receiving antenna 620 is inputted into the receiver cryptogram decoders 720. In the receiver cryptogram decoders 720it decodes by the data decoding section to which the encryption key before changing the inputted data was set.
Thenerror detection is performed.
Since the data decoding section is using different encryption keys from the encryption key which enciphered at the transmitting side in the case of data decryptionthe error of data is detected in an error detection part. If the error detected here exceeds a fixed error rateit judges that an encryption key is unusual and the encryption key currently prepared beforehand is set to the data decoding section in order. If an error rate becomes below in constant valueit can be judged that it is an encryption key after the encryption key at that time changingand it can decode correctly with the encryption key after the change after this. It is elongated with the digital image extending apparatus 730and the decoded data is changed into an analog video signaland is eventually displayed on the display 740 for image display.
[0052]Drawing 13 is a figure showing the data image in each part of a digital image broadcasting system. In a figurethe analog video signal has imagined the signal outputted from the picture reproducer 510 of the transmitting station 500. A digital compression video data is image data digitized and compressed by the digital image compression equipment 520.

Frame alignment signal F is inserted in the head of each image data.
Encryption data is an output signal of the transmitting side cryptogram decoders 530.
Each image data is enciphered with the check bit CHK of the error detecting code.
The following radio wave shows the signal until it emanates in the air and is received by the receiving antenna 620 from the transmission antenna 610.
Received data are demodulated data in the output of the tuner 710and if there is no error in a transmission line in the airthey will serve as the same signal as encryption data. The digital compression video data under it is the signal by which data decryption was carried out with the receiver cryptogram decoders 720.
It is a digital signal in the state where image data was compressed.
The compressed image data is returned with the digital image extending apparatus 730and the analog video signal shows the signal which is further changed into an analog signal and is inputted into the display 740 for image display.
[0053]Drawing 14 is a figure showing the example of composition of the transmitting side cryptogram decoders of a digital image broadcasting system. The encryption key number set part 531 to which encryption key changing instruction is inputted into the transmitting side cryptogram decoders 530 from the encryption key selecting arrangement 540 in this figureThe ROM-ized cryptograph key table 532 which two or more encryption keys are made to correspond with an encryption key numberand has been storedThe error detecting code-ized part 533 which adds a parity code to the send data from the digital image compression equipment 520It comprises the data encryption part 534 which enciphers for examplesets to DES coding LSI the send data to which the parity code was added by the encryption key corresponding to the encryption key number set up by the encryption key number set part 531. The encryption key number set part 531 comprises the external interface circuit 5311 and the encryption key latch circuitry 5312 further.
[0054]When encryption key changing instruction goes into the encryption key set part 531 of the transmitting side cryptogram decoders 530 from the encryption key selecting arrangement 540the directions are inputted into the encryption key latch circuitry 5312 via the external interface circuit 5311 of the encryption key number set part 531and are latched here. By thisan encryption key will be set as the transmitting side cryptogram decoders 530. An encryption key is selected out of the latched encryption key number using the cryptograph key table 532.
Nextwhat was error-detecting-code-ized to send data in the error detecting code-ized part 533 is put into the data coding part 534and it enciphers using the selected encryption key. The enciphered data serves as a transmission signal to the modulator 550.
[0055]Drawing 15 is a figure showing the example of composition of the receiver cryptogram decoders of a digital image broadcasting system. The data decryption-ized part 721 which the receiver cryptogram decoders 720 receive the input signal from the tuner 710for exampleis set to DES decryption LSI in this figureIt comprises the error detection part 722 which constitutes a parity check circuitthe

encryption key judgment part 723and the encryption key key table 532 of the transmitting side cryptogram decoders 530 and the ROM-ized same encryption key key table 724. The error number counter circuit 7231 which counts an error number in response to the error information from the error detection part 722 as the encryption key judgment part 723For exampleit comprises the time [ to calculate an error rate from the error number per minute ] protection circuit 7232and the key number counter circuit 7233 which changes an encryption key number one by one according to the calculated error rate.

[0056]The data decryption-ized part 721 which received the input signal is decoded with the encryption key given from the cryptograph key table 724. If that encryption key is correct at this timean input signal will be decoded correctlyand it will be changed into invalid data if the encryption key is different. The decrypted data receives a parity check by the error detection part 722and the image data except a check bit is sent out to the digital image extending apparatus 730 as received data. If an error is detected by a parity checkthe error detection part 722 will send out error information to the encryption key judgment part 723. This error information is counted in the error number counter circuit 7231and an error rate is calculated in the time protection circuit 7232. If this error rate becomes beyond a predetermined valueevery one counter value of a key number counter circuit will be made to increaseand an encryption key number will be changed one by one. Thereforeto the following input signalit will decrypt with the encryption key corresponding to this changed encryption key number.

[0057]

[Effect of the Invention]a certain incidental data being added to the data which should be enciphered in the transmitting side by this invention as having explained aboveand the incidental data being detected from data after decoding in a receiverandIf the incidental data could not detect normallyit constituted so that the encryption key of the receiver might be changed one by one. For this reasonalso when the encryption key to be used is changed and the number of the encryption key used from the transmitting side is not able to notify to a receiver normallyit can recover only by a receiver.

[0058]Since an encryption key can be changed by a receiver even if it does not transmit the number of an encryption key to a receiver positivelythe reliability and secrecy intensity of an encryption data communication system can be strengthened.

[0059]Only when a buffer means is used and normal decoding by a right encryption key is performedthe transmitted data can be altogether received correctly without lack by outputting decoding data.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a lineblock diagram showing the principle of this invention.

[Drawing 2]It is a lineblock diagram showing the 1st example of the encryption communication system of this invention.
[Drawing 3]It is a lineblock diagram showing an example of an encryption key judgment part.
[Drawing 4]It is a figure showing the data image on the transmission line of the encryption communication system of the 1st example.
[Drawing 5]It is a lineblock diagram showing the 2nd example of the encryption communication system of this invention.
[Drawing 6]It is a figure showing the data image on the transmission line of the encryption communication system of the 2nd example.
[Drawing 7]It is a lineblock diagram showing the 3rd example of the encryption communication system of this invention.
[Drawing 8]It is a figure showing the data image on the transmission line of the encryption communication system of the 3rd example.
[Drawing 9]It is a lineblock diagram showing the 4th example of the encryption communication system of this invention.
[Drawing 10]It is a figure showing the data image on the transmission line of the encryption communication system of the 4th example.
[Drawing 11]It is a lineblock diagram showing the 5th example of the encryption communication system of this invention.
[Drawing 12]It is a figure showing the example of composition which applied the encryption communication system of this invention to digital image broadcast.
[Drawing 13]It is a figure showing the data image in each part of a digital image broadcasting system.
[Drawing 14]It is a figure showing the example of composition of the transmitting side cryptogram decoders of a digital image broadcasting system.
[Drawing 15]It is a figure showing the example of composition of the receiver cryptogram decoders of a digital image broadcasting system.
[Drawing 16]It is a figure showing the composition of the conventional encryption communication system.
[Drawing 17]It is a figure showing the data image on the transmission line of the conventional encryption communication system.
[Description of Notations]
100 Sending set
101 Incidental data addition means
102 Encoding means
110 Error detecting code-ized part
120 Unique word adjunct
200 Receiving set
201 Decoding means
202 Incidental data detection means
203 Encryption key judging means
214 Error detection part
215 Encryption key judgment part

224 Unique-word-detection part
225 Encryption key judgment part